UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No.: 4:16-cr-258 CEJ (NAB)
	)	
ALDEN DICKERMAN,	)	
	)	
Defendant.	)	

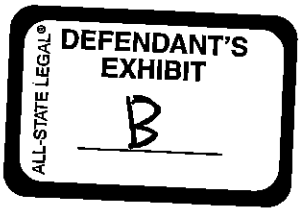
AFFIDAVIT OF STEPHEN DOUGHERTY

COMES NOW Affiant, Stephen Dougherty, and, being first duly sworn upon his oath, states and affirms the following:

1. Affiant is a natural individual of legal age and sound mind, capable of making this affidavit and personally acquainted with the facts herein stated.

2. I am a software engineer, and I have been retained by counsel for Defendant to give my expert opinion on various matters involving Freenet and the modified version of Freenet used by law enforcement. My qualifications and experience, including but not limited to: earning my Bachelor of Science in Engineering (Computer Science) Magna Cum Laude from the University of Michigan; working as a student contractor for two summers in Google Summer of Code for the Freenet Project; performing open source work for two years in the Freenet community and an additional three as the project's release manager; and skills in relevant programming languages, applications, and operating systems, make me a credible and knowledgeable source on these matters.

3. Freenet is software which provides a peer-to-peer network for censorship-resistant communication and publishing. It has anonymity protections and it is difficult to track what



information is being requested and who is requesting that information.

4. When someone runs Freenet on their computer, that instance of Freenet is called a "node."

5. Each node connects with a limited number of other nodes, and these connected nodes become each other's "peers."

6. Every node communicates with the rest of the network solely through its peers.

7. Each node has some amount of storage reserved for a "datastore"—a shared space in which each node keeps data - encrypted pieces of files.

8. Freenet allows inserting data into and fetching data from the network-wide datastore made up of all the individual nodes' datastores, which is why Freenet can be thought of as a distributed, encrypted storage device.

9. The mathematical method used by Freenet to determine which nodes to store data on, and which allows it to find that data again, is called routing.

10. I have examined documents describing the modified Freenet version (the "attack") used by law enforcement in the above-styled case to track activity and attempt to identify information and users on Freenet.

11. The attack uses a large list of suspected illegal files and the behavior of Freenet's routing to estimate the probability that received requests originated from the peer they were received from instead of forwarded through the peer from a different one, based in part on how many requests are received from the peer relative to the file's total size.

12. For the attack's estimation to be accurate, routing must be working well between the peers at that particular time.

13. The attack relies on assumptions about the node sending the requests, the node's

peers, and the quality of Internet connectivity between the peers in order to make its estimation of probability that received requests originated from the peer they were received from.

14. A number of factors can cause routing to not work as it would in ideal cases, such as when a node has a slower Internet connection than required, or a lossy Internet connection between peers, or a node recently coming online and being joined to peers with those and similar problems.

15. The routing will behave differently under such circumstances, and this can cause more requests to be sent to a node without such problems.

16. A well-equipped, high-uptime law enforcement node is a healthy candidate to receive more such requests when other peers are having the problems described above.

17. The law enforcement Freenet attack does not verify its assumptions that routing is working well. It has enough information available through normal operation to check for indications of some circumstances that can cause routing to work poorly, but aside from a check of how many peers the defendant's node reports - which suggests the attack's designers knew about this problem but made only a small effort to mitigate it - it does not make use of it.

18. If its assumption that routing is working well does not hold, this attack is not valid.

19. There is insufficient information in the warrant affidavit to evaluate the validity of the attack - whether the claim that "the number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file" is based on sound reasoning and observation. I had to read an additional paper supplied separately by the prosecutor to learn sufficient details.

FURTHER AFFIANT SAYETH NOT.

Stephen Dougherty, Affiant

Sworn to and affirmed before me on this 24 day of October, 2016

Notary Public

My Commission Expires: 04/08/2022

NOELIA PEREZ
NOTARY PUBLIC - STATE OF MICHIGAN
COUNTY OF WASHTENAW
My Commission Expires April 08, 2022
Acting in the County of Washtenaw